"Human Rights in China"
House International Relations Committee
Subcommittee on Africa, Global Human Rights and International Operations

Testimony of Ethan Gutmann
Author, Losing the New China

Wednesday, April 19, 2006, 10:30 A.M.
2172 Rayburn House Office Building.

Mr. Chairman, thank you for inviting me to make a contribution to the Committee's profoundly important work.

Approximately two months ago, your Committee heard representatives of Google, Microsoft, Yahoo, and Cisco Systems defend their companies' role in constructing China's Internet. Simultaneously the Committee floated an extremely important draft – the Global Online Freedom Act of 2006 - which appeared to place this committee and the aforementioned companies on a collision course. Some commentators, particularly those searching for a middle way, characterized the Online Freedom Act as an "overreaction." I don't agree. I believe that it is better characterized as a tragedy.

I would guess that few people in this room actually desire intrusive government intervention and oversight of U.S. companies. I certainly don't. I'm a former consultant to American corporations operating in China and a former vice-chair of the Government Relations Committee for the American Chamber of Commerce Beijing. I'm also a former believer in the concept that we would change China, not that China would change us.

But I now believe that the Internet Freedom Act may not be comprehensive enough, particularly in explicitly sanctioning Internet surveillance technologies. And I believe that the tragedy did not start with this committee but in the very early stages of American involvement in the Chinese Internet. It's the history of a collision course, not so much between Washington and American Internet companies, but between American corporate decisions and American values. We can study that history for insights into the current dilemma and potential solutions.

Two months ago, company representatives told the history of the stunning expansion of the Chinese Internet using impressive statistics – 110 million users, over 13 million bloggers – and I don't dispute them. But lost in all these figures is the simple point that Chinese Internet

freedom has actually been contracting since 1998, when I arrived in China.

Censorship was already present on the Chinese web, but dissident e-mails – spam or samizdat, depending on your perspective – flashed continuously on Chinese users' screens. Censorship didn't matter if you used proxy servers - that is, linking up to another computer that would act as an intermediary, hiding the Web footprints, evading the filters, and circumventing the government controls. The most common Chinese search words were not "Britney" and "hooters," but "free" and "proxy." About 40% of Chinese users employed proxies. A week after arriving, so did I.

A year later, working in my Beijing office, I received an e-mail from a US friend with the words "China," "unrest," "labor," and "Xinjiang" in strange half-tone brackets, as if the words had been picked out by a filter. I'd never really seen anything like it. What I didn't realize at the time is that the capability to search inside my Hotmail, primitive by the current standards, came from an American company operating in China.

During construction of the first Chinese public access web in '96, Chinese authorities suddenly became interested in blocking forbidden websites and in keyword searching - "looking into the packets."

Why? Because they are Marxists. And as my former colleague Peter Lovelock explained, that means that you must above all embrace the means of communication. Then, control it. Fill it with Chinese voices. Block the outside. And block relationships between Chinese forces.

Blocking the outside was relatively easy. Three companies were competing for the Chinanet contracts in 1997: Bay Networks, Sun Microsystems, and Cisco Systems. Cisco prevailed by selling the authorities a "firewall box" at a significant discount, which would allow the Chinese authorities to block the forbidden web.

Cisco's General Counsel denies selling any special configuration. Chinese engineers who actually worked on the firewall project are equally adamant that it was custom-made. Either way, as early as 1998, any industry-wide restraints on the transfer of censorship technologies were already being weighed against Cisco's capture of 80% of the China router market, an unprecedented success story. Yet Cisco's success may be more closely linked to a Cisco manager's statement that "We have the capability to look deeply into the packets." And I'll return to that point.

By 2000, Yahoo began censoring its search engine and patrolling chatrooms to preserve its position as the top portal in China. According

to Yahoo's former China manager: "It was a precautionary measure. The State Information Bureau was in charge of watching and making sure that we complied. The game is to make sure that they don't complain."

Let's apply that statement to more recent events. When Microsoft began suppressing words such as "democracy" and "human rights" in Chinese blogger headings, and when Google rolled out a castrated Chinese version of its search engine, company representatives made the argument that they were merely respecting local laws. Yet the laws are vague and contradictory at best; for example, the words "democracy" and "human rights" are enshrined in the Chinese constitution.

Yahoo's manager put it right the first time: "make sure that they don't complain." These were preemptive, self-censoring policies when Yahoo first employed them. They still are today. Thus any assertion that Chinese censorship is purely a government-to-government issue is premature until these companies dare to - explicitly and systematically - test the limits of Chinese laws. And until they perform that test, they should not be viewed as simply following Chinese law, but as working for Chinese Communist Party objectives.

Chinese Internet history can be divided into two periods: "before the crackdown," and "after the crackdown." From October 2000 until May 2001, the Chinese authorities unveiled new laws:

- Installation of internal monitoring software in cybercafés and across the web.

- Internet Service Providers ordered to hold all Chinese user data for 60 days.

- Proxy servers hunted and blocked.

- Construction of a national police digital network – the "Gold Shield."

The crackdown period signaled that censorship objectives were actually secondary to surveillance. Yet blocking relationships among Chinese forces – and monitoring alternate sources of political power - was far more technically demanding. For Western Internet companies the crackdown should have signaled an end to cyber-utopian illusions. Instead it signaled a new boom market for companies such as Nortel, Cisco and Sun Microsystems.

By 2003, Cisco's "Policenet" was deployed as the Internet backbone of the Chinese State Security system. Two months ago, Harry Wu exhibited slides to this committee, Cisco brochures from the Shanghai "Gold Shield" trade show in December 2002, that demonstrate the depth of Cisco's involvement with Chinese State Security. These brochures are irrefutable evidence, so I will only add three points:

- Zhou Li, a systems engineer from Cisco's Shanghai Branch, explained to me that the Cisco brochures did not give the full story. A policeman or PSB agent using Cisco equipment could now stop any citizen on the street and simply by scanning an ID card remotely access his *danwei* (work unit files): political behavior, family history, fingerprints, and other images. The agent could also access his surfing history for the last 60 days, and read his e-mail. All in real-time.

- Newly translated documents explicitly show Cisco was training the Chinese police in surveillance techniques as early as 2001.

- Detailed information on more than 96 percent of the Chinese population is now recorded on police databases, according to recent Chinese state media.

There was justifiable outrage when journalist Shi Tao received a ten-year sentence, after Yahoo surrendered his private email to Chinese security. But we really don't know how many Falun Gong practitioners, Christians, and small-time labor activists - the humdrum arrests that don't get publicized - can be attributed to Cisco's Policenet. An integrated system doesn't appear in the court records. And if recent reports are given credence, a hospital basement near Shenyang was being filled with thousands of Falun Gong practitioners for organ harvesting while Cisco was training the Chinese police.

It is my view that the situation with Cisco has already attained IBM-Holocaust status, and it will only get worse. Whether carried out by enhancements to the Online Freedom Act, or by the Commerce Department simply enforcing existing laws forbidding the sale of "crime control or detection instruments" to the Chinese police, Cisco should leave China.

I have no illusions that they will leave without a fight. By Cisco's own admission, it has contracts with Chinese State Security, at a minimum, to service equipment. Perhaps these contracts include training or upgrades as well. Yet the Israeli defense industry had an existing contract with the PLA to perform major upgrades to the Harpy Assault

Drone. Under U.S. pressure, Israel fought, but ultimately cancelled the contract. Do we have the same political will when it comes to one of our own?

Regarding Yahoo, Microsoft and Google, as I said, I consider the Online Freedom Act to be a tragedy. We did not have to reach this point.

Back in the winter of 2000, Microsoft fought the Chinese state and won. The issue was Chinese government access to foreign source codes and control of foreign encryption. Microsoft built a coalition of the American Chamber of Commerce, the US-China Business Council, the Japanese Chamber, and European entities. The US and Japanese embassies tacitly approved but avoided direct participation.

Most critically, Microsoft let it be known that if the Chinese government did not back down it would pull out of China - forever. Faced with this resolve, the Chinese government quickly chose to reinterpret their laws, i.e., they surrendered. Microsoft doesn't brag about it for obvious reasons, but I still carry that document of surrender because it shows that business has power.

So I will close by speaking about an implausible scenario: American Internet companies could form a new industry coalition, collectively ready to walk away. The Chinese authorities could agree, at a minimum, that words straight out of the Chinese constitution will never be censored by American companies. And if the Chinese police want confidential customer information from an American company, they must provide compelling evidence that the individual in question is a child pornographer.

Implausible, particularly from the American side, but far more plausible if the only other option is the Online Freedom Act: routers based outside of China, regular audits, litigation in China and at home. So companies are currently asking: what is the probability of the Online Freedom Act becoming law?

Yet the question that Microsoft, Google, and Yahoo should be focusing on is this: Will the Chinese Communist Party still be in power ten years from now? How about twenty years? And who is my primary customer base, the Chinese Communist Party or the Chinese people? Ultimately it is in American companies' self-interest to do the implausible, to form a coalition, to use their latent power, to avoid further tragedy. And I want to thank the Committee for helping to bring them closer to that point of decision.

Thank you.